CLAIM LISTING

1. (currently amended) A method for verifying authenticity of a replaceable printing component, the method comprising:

encrypting a data value stored on the replaceable printing component using a selected encryption technique to produce ~~an~~ a second encrypted data value; and

comparing the second encrypted data value with ~~an~~ a first encrypted ~~authentication~~ data value stored on the replaceable consumable whereby the replaceable printing component is authentic if the first and second encrypted data values are ~~is~~ identical ~~to the authentication value~~.

2. (original) The method of claim 1 wherein the replaceable printing component is an ink supply for an inkjet printing system.

3. (currently amended) The method of claim 1, further comprising, ~~wherein~~ prior to encrypting the data value stored on the replaceable printing component, ~~the steps of~~ encrypting the data value using a selected encryption technique to produce the first encrypted ~~an authentication~~ data value and storing each of the data value and the ~~authentication~~ first encrypted data value on the replaceable consumable ~~electrical storage device~~.

4. (currently amended) A method for storing a data value in an electrical storage device, the electrical storage device for use with a replaceable printing component, the method comprising:

encrypting the data value using a selected encryption technique to produce a first encrypted data ~~an authentication~~ value; and

storing each of the data value and the ~~authentication~~ first encrypted data value on the electrical storage device.

5. (original) The method of claim 4 wherein the replaceable printing component is an ink supply for an inkjet printing system.

6. (currently amended) The method of claim 4 further including the steps of:

encrypting a the data value stored on the replaceable printing component using a selected encryption technique to produce ~~an~~ a second encrypted data value; and

comparing the second encrypted data value with the first encrypted data an authentication value stored on the ~~replaceable consumable~~ electrical storage device whereby the replaceable printing component is authentic if the second encrypted data value is identical to the ~~authentication~~ first encrypted data value.

7. (currently amended) The method of claim 4 wherein the steps of encrypting the data value and storing each of the data value and the first encrypted data ~~authentication~~ value on the electrical storage device are performed by a processing device other than a printing system.

8. (currently amended) The method of claim 6 wherein the steps of encrypting a data value stored on the replaceable printing component and comparing the second encrypted data value with the first encrypted data ~~an authentication~~ value stored on the replaceable consumable are performed by a printing system.

9. (currently amended) The method of claim 6 further including the step of notifying customers that the replaceable printing component is not authentic if the first and second encrypted data values are ~~is~~ different ~~from the authentication value~~.

10. (currently amended) The method of claim 6 wherein the replaceable printing component is an ink supply and further including the step of providing ink from the replaceable printing component to a printing system if the first and second encrypted data values are ~~is~~ identical ~~to the authentication value~~.

11. (currently amended) A method for customizing a replaceable printing component for use in only selected printing systems, the replaceable printing component having an electrical storage device for storing data in a first portion of the electrical storage device, the method comprising:

storing a first encrypted data value ~~authentication data~~ in a second portion of the electrical storage device, the first encrypted data value derived from encrypting a data value from the first ~~data~~ portion using an encryption technique whereby prior to use of the replaceable printing component in the selected printing system requires that a resulting second encryption data value from encryption of the ~~first~~ data value using the encryption technique match the first encryption data value ~~authentication data~~ stored in the second portion of the electrical storage device.

12. (original) The method of claim 11 wherein the replaceable printing component is an ink supply and selected printing systems are inkjet printer portions.

13. (currently amended) A replaceable printing component for use in a selected printing system, the replaceable printing component including:

an electrical storage device configured for storing a data value and ~~an identifier~~ first encrypted data value, ~~the identifier value is~~ derived by encrypting the data value using an encryption process whereby upon installation of the replaceable printing component into the selected printing system the selected printing system processes the data value using the encryption process to obtain ~~an~~ second encrypted data value that is identical to the ~~identifier~~ first encrypted data value if the replaceable printing component is a verified replaceable printing component.

14. (original) The replaceable printing component of claim 13 wherein the replaceable printing component includes a supply of ink and the selected printing system is an inkjet printing system configured to receive the supply of ink.

15. (new) A method for authenticating a replaceable printing component having a memory, comprising:

with a first processing device, encrypting a data value to produce an encrypted data value and storing the data value and the first encrypted data value in the memory;

with a printing device, reading the data value from the memory, encrypting the data value to produce a second encrypted data value, comparing the first and

second encrypted data values, and taking an action according to the comparison.

16. (new) The method of Claim 15, wherein taking an action comprises taking a corrective action if the comparison reveals that the first encrypted data value is different than the second encrypted data value and initiating normal printer operation if the he comparison reveals that the first encrypted data value is not different than the second encrypted data value.

17. (new) the method of Claim 16 wherein taking a corrective action comprises issuing a notification.

18. (new) The method of Claim 15, wherein storing the first encrypted data value in the memory comprises storing the first encrypted data value in a write once portion of the memory.

19. (new) A computer readable medium having computer executable instructions for:

reading a data value from a memory provided by a replaceable printing component;

reading a first encrypted data value from the memory

encrypting the data value to produce a second encrypted data value;

comparing the first and second encrypted data values; and

taking an action according to the comparison.

20. (new) The medium of Claim 19, wherein the instructions for taking an action include instructions for taking a corrective action if the comparison reveals that the first encrypted data value is different than the second encrypted data value and initiating normal printer operation if the he comparison reveals that the first encrypted data value is not different than the second encrypted data value.